AMENDMENTS TO THE CLAIMS

Please cancel claims 2-3 without prejudice. Kindly amend claims 1, 4, 11, 14-16, 18, 22-23, 25, 28-29, 31, 34-35, 37-38, and 40 as shown in the following listing of claims. The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) An apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes ~~one of the cryptographic operations~~an encryption operation to be executed on a plurality of input text blocks that are in memory to generate a corresponding plurality of ciphertext blocks, and to store said corresponding plurality of ciphertext blocks in said memory, and wherein said cryptographic instruction also prescribes one of a plurality of block cipher modes to be employed in accomplishing said one of the cryptographic operations; and

execution logic, operatively coupled to said cryptographic instruction, configured to execute said ~~one of the cryptographic operations~~encryption operation, wherein said execution logic comprises:

a cryptography unit, ~~configured execute~~configured to execute a plurality of cryptographic rounds on each of said plurality of input text blocks to generate a corresponding ~~each of a plurality of output text blocks~~one of said corresponding plurality of ciphertext blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit, and wherein said plurality of input text blocks are retrieved from ~~memory~~said memory, and wherein said corresponding plurality of ~~output text~~ciphertext blocks are stored to said memory;

wherein said ~~one of the cryptographic operations~~encryption operation comprises:

indicating whether said ~~one of the cryptographic operations~~encryption operation has been interrupted by an interrupting event.

2. (Cancelled)

3. (Cancelled)

4. (Currently Amended) The apparatus as recited in claim 1, wherein said ~~one of the cryptographic operations~~encryption operation is accomplished according to the Advanced Encryption Standard (AES) algorithm.

5. (Cancelled)

6. (Previously Presented) The apparatus as recited in claim 5, wherein said one of a plurality of block cipher modes comprises electronic code book (ECB) mode.

7. (Previously Presented) The apparatus as recited in claim 5, wherein said one of a plurality of block cipher modes comprises cipher block chaining (CBC) mode.

8. (Previously Presented) The apparatus as recited in claim 5, wherein said one of a plurality of block cipher modes comprises cipher feedback mode (CFB) mode.

9. (Previously Presented) The apparatus as recited in claim 5, wherein said one of a plurality of block cipher modes comprises output feedback (OFB) mode.

10. (Cancelled)

11. (Currently Amended) The apparatus as recited in claim 1, further comprising:

a bit, coupled to said execution logic, configured to indicate whether said ~~one of the cryptographic operations~~encryption operation has been interrupted by said interrupting event.

12. (Original) The apparatus as recited in claim 11, wherein said bit is contained within a flags register.

13. (Original) The apparatus as recited in claim 12, wherein said flags register comprises an EFLAGS register within an x86-compatible microprocessor, and wherein said bit comprises bit 30 within said EFLAGS register.

14. (Currently Amended) The apparatus as recited in claim 1, wherein said interrupting event comprises a transfer of program control to a program flow configured to process said interrupting event, and wherein execution of said ~~one of the cryptographic operations~~encryption operation on a current input data block is interrupted.

15. (Currently Amended) The apparatus as recited in claim 14, wherein, upon return of program control to said cryptographic instruction, said ~~one of the cryptographic operations~~encryption operation is performed on said current input data block.

16. (Currently Amended) The apparatus as recited in claim 1, further comprising:

block pointer logic, operatively coupled to said execution logic, configured to direct said computing device to modify pointers to input and output data blocks in said memory to point to next input and output data blocks at the completion of said ~~one of the cryptographic operations~~encryption operation on a current input data block.

17. (Original) The apparatus as recited in claim 1, further comprising:

block pointer logic, operatively coupled to said execution logic, configured to direct said computing device to modify contents of a block counter register to indicate that said one of the cryptographic operations has been completed on a current input data block.

18. (Currently Amended) The apparatus as recited in claim 1, further comprising:

block pointer logic, operatively coupled to said execution logic, configured to direct said computing device to preserve or to generate and preserve data resulting from performance of said ~~one of the cryptographic operations~~encryption operation on a current block of data such that, upon return from said interrupting event, performance of said ~~one of the cryptographic operations~~encryption operation can continue with a following block of data.

19. (Original) The apparatus as recited in claim 1, wherein said interrupting event comprises an interrupt, an exception, a page fault, or a task switch.

20. (Original) The apparatus as recited in claim 1, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

21. (Original) The apparatus as recited in claim 1, wherein said cryptographic instruction implicitly references a plurality of registers within said computing device.

22. (Currently Amended) The apparatus as recited in claim 21, wherein said plurality of registers comprises:

a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in said memory for access of said plurality of input text blocks upon which said ~~one of the cryptographic operations~~encryption operation is to be accomplished.

23. (Currently Amended) The apparatus as recited in claim 21, wherein said plurality of registers comprises:

a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of said plurality of ~~output text~~ciphertext blocks, said plurality of ~~output text~~ciphertext blocks being generated as a result of accomplishing said ~~one of the cryptographic operations~~encryption operation upon said plurality of input text blocks.

24. (Previously Presented) The apparatus as recited in claim 21, wherein said plurality of registers comprises:

a third register, wherein contents of said third register indicate a number of text blocks within said plurality of input text blocks.

25. (Currently Amended) The apparatus as recited in claim 21, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in said memory for access of cryptographic key data for use in accomplishing said ~~one of the cryptographic operations~~encryption operation.

26. (Original) The apparatus as recited in claim 25, wherein said cryptographic key data comprises a cryptographic key.

27. (Original) The apparatus as recited in claim 25, wherein said cryptographic key data comprises a cryptographic key schedule.

28. (Currently Amended) The apparatus as recited in claim 21, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in said memory for access of an initialization vector for use in accomplishing said ~~one of the cryptographic operations~~encryption operation.

29. (Currently Amended) The apparatus as recited in claim 21, wherein said plurality of registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in said memory for access of a control word for use in accomplishing said ~~one of the cryptographic operations~~encryption operation, wherein said control word prescribes cryptographic parameters for said ~~one of the cryptographic operations~~encryption operation.

30. (Cancelled)

31. (Currently Amended) An apparatus for performing cryptographic operations, comprising:

a cryptography unit within a device, configured to execute ~~one of the cryptographic operations~~a decryption operation responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said ~~one of the cryptographic operations~~decryption operation, ~~wherein said cryptographic instruction also specifies one of a plurality of block cipher modes to be employed when performing said one of the cryptographic operations, and~~ wherein said cryptography unit is configured execute a plurality of cryptographic rounds on each of a plurality of input data blocks to generate a corresponding each of a plurality of ~~output data blocks~~plaintext blocks, and wherein said plurality of input data blocks are retrieved from memory, and wherein said plurality of ~~output data blocks~~plaintext blocks are stored to said memory;

block pointer logic, operatively coupled to said cryptography unit, configured to direct said device to modify pointers to said plurality of input and ~~output data blocks~~plaintext blocks in memory to point to next input and ~~output data blocks~~plaintext blocks at the completion of said ~~one of the cryptographic operations~~decryption operation on a current input data block; and

a bit within a register, operatively coupled to said cryptography unit, configured to indicate that execution of said ~~one of the cryptographic operations~~decryption operation has been interrupted by an interrupting event.

32. (Original) The apparatus as recited in claim 31, wherein said interrupting event comprises an interrupt, an exception, a page fault, or a task switch.

33. (Original) The apparatus as recited in claim 31, wherein said register comprises an EFLAGS register within an x86-compatible microprocessor, and wherein said bit comprises bit 30 within said EFLAGS register.

34. (Currently Amended) The apparatus as recited in claim 31, wherein said interrupting event comprises a transfer of program control to a program flow configured to process said interrupting event, and wherein execution of said ~~one of the cryptographic operations~~decryption operation on a current input data block is interrupted.

35. (Currently Amended) The apparatus as recited in claim 34, wherein, upon return of program control to said cryptographic instruction, said ~~one of the cryptographic operations~~decryption operation is performed on said current input data block.

36. (Cancelled)

37. (Currently Amended) The apparatus as recited in claim 31, wherein said block pointer logic is configured to direct said device to modify contents of a block counter register to indicate that said ~~one of the cryptographic operations~~decryption operation has been completed on a current input data block.

38. (Currently Amended) The apparatus as recited in claim 31, wherein said block pointer logic is configured to direct said device to preserve or to generate and preserve data resulting from performance of said ~~one of the cryptographic operations~~decryption operation on a current block of data such that, upon return from said interrupting event, performance of said ~~one of the cryptographic operations~~decryption operation can continue with a following block of data.

39. (Original) The apparatus as recited in claim 31, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

40. (Currently Amended) A method for performing cryptographic operations in a device, the method comprising:

fetching a cryptographic instruction from memory, wherein the cryptographic instruction prescribes one of the cryptographic operations along with one of a plurality of block cipher modes to be employed when performing the ~~one of~~one of the cryptographic operations;

retrieving a plurality of input data blocks from memory;

employing the one of a plurality of block cipher modes and executing the one of the cryptographic operations on the plurality of input data blocks to generate a corresponding plurality of output data blocks, wherein said executing is performed responsive to said fetching, ;

storing the corresponding plurality of output data blocks to the memory; and

indicating whether an interrupting event has occurred during said executing.

41. (Original) The method as recited in claim 40, wherein said indicating comprises pointing out whether an interrupt, an exception, a page fault, or a task switch has occurred during said executing.

42. (Original) The method as recited in claim 41, wherein said indicating comprises modifying the state of a bit in a register within the device.

43. (Original) The method as recited in claim 41, wherein said indicating comprises modifying the state of a bit in an EFLAGS register within an x86-compatible microprocessor.

44. (Original) The method as recited in claim 40, further comprising:

transferring program control to a program flow configured to process the interrupting event, and interrupting said executing of the one of the cryptographic operations on a current input data block.

45. (Original) The method as recited in claim 44, further comprising:

upon return of program control to said cryptographic instruction following said transferring, performing said executing on said current input data block.

46. (Previously Presented) The method as recited in claim 40, further comprising:

directing the device to modify pointers to said plurality of input and output data blocks in memory to point to next input and output data blocks at the completion of the one of the cryptographic operations on a current input data block.

47. (Previously Presented) The method as recited in claim 40, further comprising:

directing the device to modify contents of a block counter register to indicate that the one of the cryptographic operations has been completed on a current input data block.

48. (Previously Presented) The method as recited in claim 40, further comprising:

directing the device to preserve or to generate and preserve data resulting from performance of the one of the cryptographic operations on a current block of data such that, upon return from the interrupting event, performance of the one of the cryptographic operations can continue with a following block of data.

49. (Previously Presented) The method as recited in claim 40, wherein said receiving comprises:

prescribing the cryptographic instruction according to the x86 instruction format.

50. (Previously Presented) The method as recited in claim 40, wherein said receiving comprises:

prescribing an encryption operation as the one of the cryptographic operations, wherein the encryption operation comprises encryption of the plurality of input data blocks to generate the corresponding plurality of output data blocks.

51. (Previously Presented) The method as recited in claim 40, wherein said receiving comprises:

prescribing a decryption operation as the one of the cryptographic operations, wherein the decryption operation comprises decryption of the plurality of input data blocks to generate the corresponding plurality of output data blocks.

52. (Original) The method as recited in claim 40, wherein said executing comprises:

accomplishing the one of the cryptographic operations according to the Advanced Encryption Standard (AES) algorithm.

53. (Cancelled)

54. (Currently Amended) The method as recited in claim 53, wherein the one of a plurality of block cipher modes comprises electronic code book (ECB) mode.

55. (Currently Amended) The method as recited in claim 53, wherein the one of a plurality of block cipher modes comprises cipher block chaining (CBC) mode.

56. (Currently Amended) The method as recited in claim 53, wherein the one of a plurality of block cipher modes comprises cipher feedback mode (CFB) mode.

57. (Currently Amended) The method as recited in claim 53, wherein the one of a plurality of block cipher modes comprises output feedback (OFB) mode.